

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED Top Secret b. LEVEL OF SAFEGUARDING REQUIRED None	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)				3. THIS SPECIFICATION IS: (X and complete as applicable)	
<input type="checkbox"/>	a. PRIME CONTRACT NUMBER			<input type="checkbox"/>	a. ORIGINAL (Complete date in all cases)
<input type="checkbox"/>	b. SUBCONTRACT NUMBER			<input type="checkbox"/>	b. REVISED (Supersedes all previous specs)
<input checked="" type="checkbox"/>	c. SOLICITATION OR OTHER NUMBER GSC-QF0B-16-33016		DUE DATE (YYYYMMDD) 2016XXXX	<input type="checkbox"/>	c. FINAL (Complete Item 5 in all cases)
DATE (YYYYMMDD) 2016XXXX					
4. THIS IS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip code)	
8. ACTUAL PERFORMANCE					
a. LOCATION		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
See Continuation Page					
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT The requested services shall be provided by Logistics Readiness Center, Directorate of Readiness, Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Systems Operations, Installation, Logistics, Training, Maintenance, and related sustainment support.					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:			11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		
	YES	NO		YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input checked="" type="checkbox"/>	<input type="checkbox"/>
b. RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input type="checkbox"/>	<input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION:	<input type="checkbox"/>	<input type="checkbox"/>	e. PERFORM SERVICES ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) Sensitive Compartmented information (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input checked="" type="checkbox"/>	<input type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	<input type="checkbox"/>	<input checked="" type="checkbox"/>
g. NATO INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS	<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER (Specify)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
k. OTHER (Specify) SIPRNET, NSANet SCGs, NIPRNet (see Continuation Page)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	IT sensitive duties required (see Continuation Page), SCI IS Processing required (See Appendix B, Item 8)	<input type="checkbox"/>	<input type="checkbox"/>

12. PUBLIC RELEASE. Any information (*classified or unclassified*) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☒ Through (*Specify*): **SCI NOT AUTHORIZED FOR RELEASE AT ANY TIME**

Release of other than SCI through CECOM Logistics and Readiness Center, Attn: AMSEL-LCF-F (Mike Pettitt) Aberdeen Proving Ground, MD 21005 and CECOM G2 OPSEC Officer, Edward Eilerman, Jr. 443-861-5554, Edward.eilerman2.civ@mai.mil, TO APG Public Affairs Office, APG, MD, 21005

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (*Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*)

Period of Performance: Task Order Start Date – XX September 2016 through a one-year base period, plus four one-year option periods

CO: Odis Kenton, GSA FAS, FEDSIM, 1800 F Street NW Suite 3100, Washington, DC 20405 (703)-244-0309, odis.kenton@gsa.gov

COR: Kelly Swain, GSA FAS, FEDSIM, 1800 F Street NW Suite 3100, Washington, DC 20405 (703)-539-9647, kelly.swain@gsa.gov

TPOC: **TBD**

CECOM Security Officer: **TBD**

SECURITY REVIEW BY: Kandis Yount, GSA, FAS, FEDSIM Security Manager DATE:

Section 13 continued in Attachment One, Security Guidance

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☒ Yes ☐ No
(*If Yes, identify pertinent contractual clauses in the contract document itself, or provide any appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.*)

See SCI Addendum, Appendix B

Program protection plans will be provided as government furnished information if CPI is identified.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☒ Yes ☐ No
(*If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.*)

Contractor personnel performing OCONUS will be serviced by the Servicing Security Activity (SSA) for the country being visited. The SSO is responsible for inspection and oversight of SCIF at Government Facilities. DCS, G-2 will provide oversight to ensure program protection plans implementation and CPI protection.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL
Odis Kenton

b. TITLE
Contracting Officer

c. TELEPHONE (*Include Area Code*)
(703)-244-0309

d. ADDRESS (*Include Zip Code*)
1800 F Street NW Suite 3100
Washington, DC 20405

e. SIGNATURE

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
- ☐ b. SUBCONTRACTOR
- ☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- ☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- ☒ e. ADMINISTRATIVE CONTRACTING OFFICER
- ☒ f. OTHERS AS NECESSARY

ATTACHMENT ONE
ADDENDUM TO DD 254
ITEM # 13 (CONTINUED), SECURITY GUIDANCE

8a: ACTUAL PERFORMANCE: Complete revised DD254 packages must be submitted for all additional locations of performance that are not listed on this Award/Task Order DD254 package. This includes prime contractor, subsidiaries, subcontractors, and government facilities. Submit the revisions through the CO for review, signature and approval. All contractors and subcontractors require TOP SECRET facility clearances and NO safeguarding. All personnel must be US citizens. Dual citizenship status not authorized.

Additional Performance Locations

Performance will take place at CONUS and OCONUS locations. Performance for Task 1 will be at the contractor's site.

For Tasks 3 through 9, the current places of performance are as follows:

- a. **401st AFSB (SWA)** – Bagram, Fenty, Gamberi, Jalalabad, Kandahar, Kaia, Morehead, New Kabul Compound, Qargha, Dwyer, Herat, and Camp Dahlke in Afghanistan; Camp Arifjan and Camp Buhering in Kuwait; and, Al Taqqadum (TQ), Camp Swift, and Taji in Iraq
- b. **403rd AFSB (Korea)** – Camp Humphreys and Camp Stanley
- c. **404th AFSB (CONUS Pacific)** – JBLM, Washington and Schofield Barracks, Hawaii
- d. **405th AFSB (Europe)** – Kaiserslautern, Germany; Vicenza, Italy; Camp Lemonier, Djibouti; and, North Camp and El Gorah in Egypt
- e. **406th AFSB (CONUS East)** – Fort Bragg, North Carolina; Fort Campbell, Kentucky; and, Redstone Arsenal in Huntsville, Alabama
- f. **407th AFSB (CONUS West)** – Fort Hood and Fort Bliss in Texas

For Task 10, the current places of performance are as follows:

- a. **Section C.5.10.1**, C4ISR Systems Maintenance Data Tracking and Reporting Support – APG, Maryland
- b. **Section C.5.10.2**, Army Watercraft System Support – APG, Maryland
- c. **Section C.5.10.3**, LRC PED Support – Letterkenny Army Depot, Pennsylvania
- d. **Section C.5.10.4**, ASLAC Support – Charleston, South Carolina
- e. **Section C.5.10.5**, DPAA Support, Hawaii – Pearl Harbor, Hawaii
- f. **Section C.5.10.6**, DPAA Support, Europe – Miesau, Germany
- g. **Section C.5.10.7**, COSIS Support – Fort Bragg, North Carolina and Fort Bliss, Texas
- h. **Section C.5.10.8**, USAISEC Support – Kaiserslautern, Germany

Any additional (new) locations (except short duration deployments on temporary duty status) shall be added to this task order by formal task order modification (amendment).

10a: COMSEC: COMSEC material may not be released to DoD contractors without CECOM approval. Contractor must forward request for COMSEC material/information to the COMSEC officer through the Program Office. The contractor is governed by the DoD 5222.22-S COMSEC Supplement to the NISPOM in the control and protection of COMSEC material/information. Access to COMSEC material by personnel is restricted to U.S. citizens holding final U.S. Government clearances. Such information is not releasable to personnel holding only reciprocal clearances. Classified COMSEC material is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. COMSEC access shall be IAW DoD 5220.22-M, Chapter 9, Section 4, AR 380-40 and Additional Security Guidelines for COMSEC, Appendix A. When access is required at Government facilities, contractor personnel will adhere to COMSEC rules and regulations as mandated by Command policy and procedures.

Concurrence of the KO is required prior to subcontractors working on the program. Copies of the subcontract DD Form 254 will be forwarded to the KO for the Contract file and to CECOM G2 for DD Form 254 tracker information. Per AR 380-40, Chapter 4: Contractor personnel are subject to the Department of Army Cryptographic Access Program (DACAP).

10e (1): SENSITIVE COMPARTMENTED INFORMATION: All contractor SCI work and access will be at a designated Government SCIF. The contractor must have SCI indoctrinated personnel available to work the contract. All contract personnel requiring access to SCI material must be U.S. citizens, have been granted a final Top Secret security clearance by the U.S. Government, have been approved as meeting DCID 6/4 criteria by a Government Cognizant Security Authority (CSA), and have been indoctrinated for the applicable compartments of SCI accesses prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis are not eligible for access to intelligence information released or generated under this contract. Classified material released or generated under this contract is not releasable to foreign nationals without the expressed written permission of CECOM. Prior approval of the Contracting Officer is required for subcontracting. See attached SCI Release of Intelligence Information for additional security requirements.

10e(2): NON-SCI: See attached non-SCI release of Intelligence Information for additional security requirements. Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a final U.S. Government clearance at the appropriate level. Written concurrence of the KO is required prior to subcontracting.

10g NATO INFORMATION: The contractor is authorized access to documents belonging to and circulated by the North Atlantic Treaty Organization (NATO). Access to NATO information by the contractor will occur at government facilities only. Access to NATO requires a final U.S. Government clearance at the appropriate level. A representative of the Government will brief the Facility Security Officer (FSO), who in turn will brief other contractor personnel requiring access under the contract.

Personnel not assigned to a NATO staff position, but requiring access to NATO classified information, NATO Secret or access to the NATO accredited SIPRNET terminals, must possess the equivalent FINAL U.S. Security Clearance based upon the appropriate personnel security investigation required. Personnel with access to NATO ATOMAL information must have the appropriate level FINAL U.S. Security Clearance. The government program/project manager is the designated representative that will ensure the contractor security manager and concerned employees are NATO briefed prior to access being granted. The contractor will maintain strict compliance in regards to NATO information IAW NISPOM Ch 10, Section 7. Prior approval from the KO is required for subcontracting. All Contractor facilities approved for SCI Networks must send a copy of the Facility Checklist, Co-Use Agreements, MOA/MOUs and Facility and Network Accreditations documents to CECOM G2, Industrial Security.

10j: FOR OFFICIAL USE ONLY (FOUO) INFORMATION: FOUO Information provided under this contract shall be safeguarded as specified in DoD 5400.7-R, "Protecting For Official Use Only (FOUO) Information." Also, see attached instructions on "For Official Use Only (FOUO) Information." Safeguarding "For Official Use Only" (FOUO) information. FOUO Information generated and/or provided under this contract shall be safeguarded and marked as specified in AR 25-55 and DoD 5200.1

10k: OTHER: NSANET access required. All contractors requiring access to NSANET MUST have a final Top Secret clearance and be indoctrinated for Sensitive compartmented Information access. Contractors and/or Subcontractors requiring access to the NSANET will require a successfully completed Full Scope (Lifestyle) or Counterintelligence Polygraph. Contractors requiring access to NSANET receive a COMSEC briefing prior to being granted access to NSA NET. All Contractor facilities approved for SCI Networks must send a copy of the Facility Checklist, Co-Use Agreements, MOA/MOUs and Facility and Network Accreditations documents to CECOM G2, Industrial Security.

The contractor will require access to the following security classification guides:

- The Joint Counter Radio Controlled Improvised Explosive Device Electronic Warfare (JCREW) Program SCG dated April 2, 2007 (FOUO); available for anyone with Army Knowledge Online (AKO) account at <https://www.milsuite.mil/book/docs/DOC-133118>.
- DoD CREW: Interim Classification Guidance - Universal Classification Reference Matrix, September 2, 2008 (FOUO); <https://www.milsuite.mil/book/docs/DOC-269067>.
- DoD CREW: Interim Classification Guidance – Compilation, December 22, 2014 (FOUO); <https://www.milsuite.mil/book/docs/DOC-179731>.

Contractor requires access to the Rapid Aerostat Initial Deployment (RAID) Systems Security Classification Guide (SCG) dated 20 Feb 2014. SIPRNET ACCESS: All contractors requiring access to the SIPRNET MUST HAVE A FINAL SECRET CLEARANCE OR Interim Top Secret clearance. All contractors with SIPRNET access MUST receive COMSEC and NATO Awareness briefings from their FSO prior to being granted access. COMSEC and NATO Awareness Briefing dates must be recorded on all visit requests. The NATO Awareness Briefing is required to inform personnel how to protect NATO information in the event they come across it while accessing SIPRNET. The contractor shall not access, download or further disseminate any special access data (i.e., intelligence, NATO, COMSEC, etc.) outside the execution of the defined contract requirements. All contractors will read the NATO Central Registry awareness briefing located at: <https://secureweb.hqda.pentagon.mil/cusr/forms.aspx> prior to being issued a SIPRNet account. This briefing does not authorize NATO access, and is solely for the purpose of awareness. Access to SIPRNet is required at Government facilities only. All contractors granted SIPRNet access must be aware that they are not authorized to download ANY classified material without the guidance and written permission of the Cognizant Security Agency.

11a: HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTORS FACILITY OR GOVERNMENT ACTIVITY: This means that the contractor does not require “Safeguarding” capability at its facility and there will be no access to Classified National Security Information (CNSI) at the contractor’s facility. Classified performance is restricted to Government facilities. Government agency or activity will provide security classification guidance for performance of this contract. Submit visit request to the KO and/or Security Management Office for need-to-know verification.

11f: HAVE ACCESS TO US CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES: A copy of the DD 254 must be provided to the Office of Security Services International (OSSI) or other U.S. activity responsible for overseas inspections. See 8a above.

11g: BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER: Per NISPOM Chapter 11, Section 2 Contractor must submit DD form 1540 and DD Form 2345 for registration with DTIC. Technical information on file at the DTIC will be made available to contractor if the contractor requires such information. The contracting officer will certify the field of interest relating to the contractor. Contractor generated or Government furnished materials may not be provided to the Defense Technical Information Center (DTIC). Contract generated technical reports will bear the statement “NOT RELEASABLE TO THE DEFENSE TECHNICAL INFORMATION CENTER PER DOD INSTRUCTIONS 5230.24.

The contractor is authorized the use of the Defense Technical Information Center (DTIC) or other secondary distribution center. The contractor will prepare DD Forms 1540 and 2345 for authorized access to DTIC. Completed forms will be provided to the KO for processing.

11j: HAVE OPERATION SECURITY (OPSEC) REQUIREMENTS: OPSEC is a structured process that identifies critical information, analyzes friendly actions, integrates threat analysis and risk assessments, then helps personnel apply protective measures to mitigate unacceptable risk. Organizations and personnel supporting CECOM may have OPSEC requirements associated with their activities and support. The contractor will comply CECOM OPSEC Program. The basis for the on-site contractor

OPSEC program is the IAW AR 530-1, Chapter 6 as listed in the PWS CDRL A035 and Project Manager Electronic Warfare (PM EW) OPSEC Plan, Version 3.0, dated May 2013. CECOM is the Government facility OPSEC point of contact. OPSEC requirements apply. The contractor must comply with special OPSEC requirements contained in the contract or addendum thereto. The following standard expectations are included in all work.

- a. The contractor supporting specific event-oriented activities will develop OPSEC Plans/Annexes when directed by the supported program, or comply with the program's OPSEC Plan/Annex.
- b. Personnel assigned will receive OPSEC Awareness Education and Duty-Related Training as deemed necessary by the Government or program supported.
- c. OPSEC Awareness Education and Training will be provided or coordinated through government channels.

Contractor shall adhere to the OPSEC requirements IAW the following Program OPSEC Plan/SOP: (Product Management Office, Electro-Optical/ Infrared Payloads – Force Protection, Operations Security Program, dated June 2014), as listed in the PWS CDRL A001.1

11I: OTHER: SCI IS Processing required (See Appendix B, Item 8). All classified systems authorized at contractor facilities MUST be accredited prior to the start of processing Classified Network requirement.

13a. Contractor personnel performing IT sensitive duties are subject to investigative and assignment requirements IAW AR 25-2, AR 380-67, DoD 8570.0 and affiliated regulations. Army regulation available at www.apd.army.mil

13b. Foreign subcontractors, foreign vendors and/or visitors that are not cleared US Companies, participating in Army foreign disclosure issues will be handled in accordance with AR 380-10, Appendix G, para G-4. Foreign subcontractor participation will be handled in accordance with AR 380-10 (Technology

Transfer, Disclosure of Information & Contacts with Foreign Representatives), (DTM) 09-019 - "Policy Guidance for Foreign Ownership, Control, or Influence (FOCI)", September 2, 2009, National Disclosure Policy, and affiliated regulations and/or supplements and AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, dated 4 DEC 2013.

- All disclosures (i.e. oral, visual, briefing, documents) to foreign nationals require prior approval by the foreign disclosure officer.
- All requests for non-US cleared Foreign subcontractor and/or Foreign own companies to perform on this contract must be requested from the Prime Contract to the CO through Program Office and approved by Foreign Disclosure Officer

13c. Classified information will be protected IAW the NISPOM, Chapter 5. All security incidents involving classified information will be reported to the CECOM G2 Industrial Security Office, and DSS Industrial Security Representative. Information will be forwarded to CO and the PM for a program damage assessment to be conducted IAW AR 380-49

13d. All subcontractor DD254s and subcontractor tier DD254s will be sent to the CO. Any Contractors/subcontractors owned by Foreign Companies and that have a clearance issued by the Defense Security Service under a Special Security Agreement need to have a National Interest Determination (NID) approved if access is required to: Top Secret; COMSEC; Restricted Data; SCI and/or SAP. NID requirements and justification must be sent through CECOM G2 to be forwarded to the approving agencies. Only after a NID approval is received will a FOCI contracting firm be authorized to work on the program.

13e. The contractor FSO will include Threat Awareness and Reporting Program (TARP) requirements in their initial and refresher training IAW AR 381-12, paragraph 1-14 and Chapter 2.

13f. The contractor must submit subcontracts to DD254's to the CO for the contract file and forward to CECOM G2 for review to insure Army requirements flow down to the subcontractor.

13g. All Facility Clearance sponsorships for subcontractors must have Government approval and certification on the subcontractor's DD 254. Submit all requests to the CECOM G2 security office.

13h. Record of security-related training of contractors and embedded contractors must be available for review.

Certification and Signature: Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

14: REPORTS: In addition to the reporting requirements in para 1-302 of the NISPOM, the Contractor Facility Security Officer shall provide a copy of any report submitted to the Cognizant Security Agency (CSA) to the CECOM Security Office identified in Block 13 within one (1) business day of submitting the report to the CSA.

14: Ref 10e(1). See attached SCI Release of Intelligence Information for additional security requirements. Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a final U.S. Government clearance at the appropriate level.

14: Ref 10e(2). See attached non-SCI release of Intelligence Information for additional security requirements. Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a final U. S. Government clearance at the appropriate level.

OTHER:

**ATTACHMENT TWO
ADDENDUM TO DD 254**

US ARMY SCI ADDENDUM TO DD FORM 254, 31 May 2005

XXX (1) This contract requires access to Sensitive Compartmented Information (SCI). The Commander, US Army Intelligence and Security Command (INSCOM), acting on behalf of the DA Deputy Chief of Staff (DCS), G-2 as the Cognizant Security Authority (CSA) for the US Army, has exclusive security responsibility for all SCI released to the contractor or developed under the contract and held within the Contractor's SCI Facility (SCIF) or Co-utilization Agreement (CUA) SCIF. The Defense Intelligence Agency (DIA) has security inspection responsibility for SCI and the Defense Security Service (DSS) retains responsibility for all collateral information released or developed under the contract and held within the DoD Contractor's SCIF. The manuals, regulations and directives checked below provide the necessary guidance for physical, personnel, and information security for safeguarding SCI, and are part of the security classification specification for this contract:

XXX ☐ DoD 5105.21-M-1, SCI Security Manual, Administrative Security

XXX ☐ Signals Intelligence Security Regulations (SISR) (Available from the CM)

XXX ☐ Imagery Policy Series (Available from the CM)

☐ DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems

☐ DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities

XXX ☐ AR 25-2, Information Assurance

XXX ☐ AR 380-28, DA Special Security System

☐ AR 380-381, Special Access Programs (SAPS).

XXX ☐ Army Handbook for SCI Contracts.

☐ Other

XXX (2) Contract estimated completion date: Task Order Start date - **XX September 2016** with a one-year base period and four, one-year option periods.

XXX (3) The name, telephone number, email address and mailing address of the Contract Monitor (CM) for the SCI portion of this contract is: SCI CM: Channing Wooten 443 861 6369 DSN 848 Logistics Readiness Center ATTN: AMSEL-LCR-F, Aberdeen Proving Ground, MD 21050 Channing.c.wooten2.civ@mail.mil

SCTY POC: TBD

XXX (4) All DD Forms 254 prepared for subcontracts involving access to SCI under this contract must be forwarded to the CM for approval and then to HQ INSCOM, ACofS Security, G2, Contractor Support Element (CSE) for review and concurrence prior to award of the subcontract.

XXX (5) The contractor will submit the request for SCI visit certifications through the CM for approval of the visit. The certification request must arrive at the Contractor Support Element at least ten (10) working days prior to the visit. Visit certification requests will be processed through ACAVS.

XXX (6) The contractor will not reproduce any SCI related material without prior written permission of the CM.

XXX (7) Security Classification Guides or extracts are attached or will be provided under separate cover.

XXX (8) Electronic processing of SCI requires accreditation of the equipment in accordance with DCID 6/3 and AR 25-2 (Note: Check only if item 11I indicates that a requirement exists for SCI IS processing.)

☐ (9) This contract requires a contractor SCIF.

XXX (10) This contract requires ☐ (SI) ☐ (TK) ☐ (G) ☐ (HCS) (Add others as required)

XXX (11) The contractor will perform SCI work under this contract at the following locations: SEE NEXT PAGE

SCI Addendum Continued

(11) Continued: The contractor will perform SCI work under this contract at but not limited to the following locations:

- a. Continental United States (CONUS) including Fort Bragg, North Carolina; Fort Campbell, Kentucky; Fort Hood, Texas;; Fort Bliss, Texas; Joint Base Lewis-McChord, Washington; Aberdeen Proving Grounds, Maryland; Letterkenny Army Depot, Pennsylvania; the Army Strategic Logistics Activity Charleston (ASLAC); the National Training Center (NTC); Fort Irwin, California; the Joint Readiness Training Center (JRTC; Fort Polk, Louisiana); and the National Capital Region.
- b. Outside the Continental United States (OCONUS) including Alaska, Hawaii, Europe / NATO nations, Republic Of Korea, Kuwait, Afghanistan, Qatar, Oman, Saudi Arabia, and Djibouti (and other AFRICOM base locations in Africa as may be established), Kosovo and Egypt (including the Sinai Peninsula),
- c. Any additional (new) locations (except short duration deployments on temporary duty status) shall be added to this task order by formal task order modification (amendment). A DD Form 254 revision will be required for any new locations.

**ATTACHMENT THREE
ADDENDUM TO DD 254**

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Provided by the CECOM LCMC Director of Intelligence & Security/G2
(Updated: 14 July 2008)

Contractor Generated Communications Security (COMSEC) Material: Any material generated by the contractor (including, but not limited to: correspondence, drawings, models, mockups, photographs, schematics, status programs and special inspection reports, engineering notes, computations and training aids) will be classified according to its own content. Classification guidance will be taken from other elements of this Contract Security Classification Specification, DD Form 254, Government furnished equipment or data, or special instructions issued by the Contracting Officer, or his/her duly appointed representative.

REQUIREMENTS:

1. The requirements of DoD 5220.22-M and NSA/CSS Policy Manual 3-16 are applicable to this effort.
2. All contractor personnel to be granted access to classified COMSEC information must be U.S. citizens granted FINAL clearance by the government prior to being given access. Immigrant aliens, interim cleared personnel, or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified COMSEC information released or generated under this contract without the express permission of the Director, NSA.
3. Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring contracting officer.
4. No contractor generated COMSEC or government furnished material may be provided to the Defense Technical Information Center (DTIC). Contractor generated technical reports will bear the statement "Not Releasable to the Defense Technical Information Center per DoD Directive 5100-38."
5. Classified paper COMSEC material may be destroyed by burning, disintegration, chopping or high security crosscut shredding. Cryptographic key tapes must be "terminally" destroyed (destroyed to the point where it cannot be reconstructed) utilizing devices listed on the Evaluated Products List (EPL) for Punched Tape Destruction Devices or the EPL for High-Security Disintegrators. A listing of EPLs can be found at <http://www.nsa.gov/ia/government/mdg.cfm>. When a method other than burning is used, all residue must be reduced to pieces 5mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.
6. Unclassified COMSEC information released or generated under this contract shall be restricted in its dissemination to personnel involved in the contract. Release in open literature or exhibition of such information without the express written permission of the Director, NSA, is strictly prohibited.
7. Recipients of COMSEC information under this contract may not release information to subcontractors without permission of the User Agency.
8. Additional notices to be affixed to the cover and title or first page of contractor generated COMSEC documents:
 - a. "COMSEC MATERIAL - ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE."

b. "THIS PUBLICATION OR INFORMATION IT CONTAINS MAY NOT BE RELEASED TO FOREIGN NATIONALS WITHOUT PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA. ALL APPROVALS WILL IDENTIFY THE SPECIFIC INFORMATION AND COPIES OF THIS PUBLICATION AUTHORIZED FOR RELEASE TO SPECIFIC FOREIGN HOLDERS. ALL REQUESTS FOR ADDITIONAL ISSUANCES MUST RECEIVE PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA."

9. Point of contact is CECOM LCMC G2, ATTN: AMSEL-MI.

**ATTACHMENT FOUR
ADDENDUM TO DD 254**

**INTELLIGENCE MATERIALS ACCESS REQUIREMENTS
Provided by CECOM LCMC G2
(Updated: 14 July 2008)**

1. No Intelligence materials are to be provided in support of the contract without the prior approval of the FEDSIM Contracting Officer (CO) and CECOM Life Cycle Management Command (CECOM LCMC) G2 Director of Intelligence and Security. Any intelligence materials so provided will be disseminated solely by the CECOM LCMC G2, and will be accompanied by both a Letter of Instruction governing control of the materials provided, and a Letter of Transmittal, identifying the materials loaned and the duration of the loan. This service only pertains to elements supported by the CECOM LCMC G2.
2. All requests for access to intelligence materials will adhere to the following guidelines:
 - a. Prime contractor requests for intelligence materials access will be sent to the Program/Project Manager (PM) of the User Activity on official business letterhead with an enclosed copy of the approved DD Form 254.
 - b. Subcontractor requests for access to intelligence materials will be forwarded by the prime contractor to the PM on official business letterhead with an enclosed, approved DD Form 254 for the relevant subcontract.
 - c. PM of the User Activity will forward request through the Contracting Officer (CO) on official letterhead with the appropriate DD Form 254 and all substantiating documents attached, to be forwarded to the CECOM LCMC G2 for review and concurrence.
3. Point of contact is CECOM LCMC G2, AMSEL-MI (ATTN: Current Intelligence).

**ATTACHMENT FIVE
ADDENDUM TO DD 254**

SAFEGUARDING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION

Provided by the CECOM Director of Intelligence & Security/G2

(Updated: 14 July 2008)

Reference: AR 25-55, Chapter IV

1. The "FOR OFFICIAL USE ONLY" marking is assigned to information at the time of its creation in a DOD User Agency. It is not authorized as a substitute for a security classification marking but it is used on official Government Information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act.
2. Other non-security markings such as "Limited Official Use" and "Official Use Only" are used by non-DOD User Agencies for the same type of information and should be safeguarded and handled in accordance with instructions received from such agencies.
3. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release, to determine whether a significant and legitimate Government purpose is served by withholding the information or portions of it.

4. IDENTIFICATION MARKINGS:

a. An unclassified document containing FOUO information shall be marked "For Official Use Only" in bold letters at least 3/16 of an inch high at the bottom of the front cover (if any), on each page containing FOUO information, and on the outside of the back cover (if any). No portion marking will be shown.

b. Within a classified document, an individual page that contains both FOUO and classified information will be marked at the top and bottom with the highest security classification appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked 'FOUO.'

c. Any "FOR OFFICIAL USE ONLY" information released to a contractor by a DOD User Agency is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA.
EXEMPTIONS APPLY.

d. Removal of the "FOR OFFICIAL USE ONLY" marking can only be accomplished by the originator or other competent authority. When "FOR OFFICIAL USE ONLY" status is terminated, all known holders will be notified to the extent possible.

5. DISSEMINATION: Contractors may disseminate "FOR OFFICIAL USE ONLY" information to their employees and subcontractors who have a need for the information in connection with a classified contract.

6. STORAGE: During normal working hours "FOR OFFICIAL USE ONLY" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks is adequate when internal building security is provided during non-working hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.

7. TRANSMISSION: "FOR OFFICIAL USE ONLY" information may be sent via first-class mail or parcel post. Bulky shipments may be sent fourth-class mail.

8. DISPOSITION: When no longer needed, FOUO information may be disposed of by tearing each copy into pieces to preclude reconstructing, and placing it in a trash container or as directed by the User Agency.
9. UNAUTHORIZED DISCLOSURE: Unauthorized disclosure of "FOR OFFICIAL USE ONLY" information does not constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.
10. Point of contact is CECOM LCMC Director of Intelligence & Security/G2, ATTN: AMSEL-MI.